Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re: Clearview AI, Inc. Consumer Privacy Litigation	Case No. 1:21-cv-00135 Hon. Sharon Johnson Coleman

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Constitution and our nation's civil rights laws. The ACLU of Illinois is a state affiliate of the ACLU. Both organizations have been at the forefront of efforts nationwide to protect the full array of civil rights and liberties, including the rights to free speech and biometric privacy. The ACLU and ACLU of Illinois have frequently appeared before courts throughout the country in First Amendment cases and in cases concerning Illinois' Biometric Information Privacy Act, both as direct counsel and as amici curiae. *See, e.g., ACLU v. Clearview AI*, No. 2020 CH 04353 (Ill. Cir. Ct., Cook Cty. filed May 28, 2020) (counsel); *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (amicus); *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019) (amicus); *ACLU of Ill. v. Alvarez*, 679 F.3d 583, 586 (7th Cir. 2012) (counsel); *see also ACA Connects - Am.'s Commc'ns Ass'n v. Frey*, 471 F. Supp. 3d 318 (D. Me. 2020) (amicus brief explaining why state law protecting privacy of internet use records is subject to First Amendment scrutiny and survives such scrutiny).. The application of the correct First Amendment scrutiny to biometric privacy laws, including BIPA, is therefore of immense concern to amici, their clients, and their members and donors.

[1] Amici confirm that no party or counsel for any party authored this brief in whole or in part, that no person other than amici or their counsel made any monetary contribution intended to fund the preparation or submission of this brief, and that Plaintiffs consent to and Defendants do not oppose the filing of this brief.

INTRODUCTION

Surreptitiously, and without consent, Defendant Clearview AI, Inc. ("Clearview") has captured the unique biometric identifiers of countless Illinoisans, and used them to amass what it calls the "world's best facial recognition technology combined with the world's largest database of headshots."[2] The size of Clearview's database dwarfs that of other face recognition systems.[3] Public reporting indicates that Clearview has offered its tool to thousands of entities and individuals, including celebrities, wealthy businesspeople, individual police officers, corporate employees, and more than 200 companies.[4] The technology has been used for everything from enabling a billionaire to identify his daughter's date at a restaurant, to "demonstrations of its power for fun" at parties, during business gatherings, and among kids,[5] to identifying individuals

---

[2] Thomas German, *Why Illinois Has Become a Battleground for Facial Recognition Protection*, Consumer Rep. (May 29, 2020), https://www.consumerreports.org/privacy/why-illinois-has-become-a-battleground-for-facial-recognition-protection/.

[3] *See* U.S. Gov't Accountability Off., *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* 16 (June 2021), https://www.gao.gov/assets/gao-21-518.pdf [hereinafter "GAO Facial Recognition Risks Report"].

[4] Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By the Justice Department, ICE, Macy's, Walmart, And the NBA*, BuzzFeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement (revealing Clearview's work with over 2,200 police and law enforcement agencies, individuals, and retailers, spanning 26 countries and the U.S.); *see also* Ryan Mac, Caroline Haskins, Brianna Sacks & Logan McDonald, *Your Local Police Department Might Have Used this Facial Recognition Tool to Surveil You. Find Out Here*, BuzzFeed News (Apr. 9, 2021), buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table (detailing use by individual government employees, including at least 34 organizations that "said they were unaware that their employees had signed up for free trials until [the reporters'] questions prompted them to look" and 69 entities that "at first denied their employees had used Clearview but later determined that some of them had").

[5] Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 6, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.

during last summer's historic protests against racist police brutality.[6]

To run its face recognition tool, Clearview captures "faceprints," or scans of facial geometry, which it refers to as "facial vectors," *see* Def. Mem. Supp. MTD at 10 [hereinafter "Def. MTD"], from images across the Internet without the pictured individuals' knowledge or consent. Faceprints are biometric identifiers—measurements of our immutable and unique biological characteristics—akin to fingerprints or DNA profiles. Like fingerprints, they are "prints" of our body parts, calculated by measuring our physical geometry. Fingerprints are measures of our fingers' loops, whorls, and ridges; faceprints are measures of the vectors between certain points on our faces.

Faceprints and other biometric identifiers can be used to discern identity and to grant access to secure locations, accounts, and information. And, unlike a social security or passport number, they cannot be changed or protected once control is lost. In the words of the Illinois legislature, biometric identifiers are "biologically unique to the individual; therefore, once compromised, the individual has no recourse, [and] is at heightened risk for identity theft" and other privacy and security harms. 740 ILCS 14/5(c). Nonconsensual capture thus presents serious privacy and security risks.

Illinois has taken steps to curb such abuses. Passed in 2008, the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14, requires entities to provide notice to and obtain informed

[6] *See* Connie Fossi & Phil Prazan, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC Miami (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/; GAO Facial Recognition Risks Report, *supra* n.3 at 18 (detailing U.S. Postal Inspection Service use of Clearview AI during "civil unrest, riots, or protests"); Juliette Rihl, *Emails Show Pittsburgh Police Officers Accessed Clearview Facial Recognition After BLM Protests*, PublicSource (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview/.

written consent from individuals before collecting their biometric identifiers, including faceprints. These protections, which the Illinois Supreme Court has described as "particularly crucial in our digital world," *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 34, 129 N.E.3d 1197, 1206, ensure that Illinoisans retain control over their biometric identifiers.

There can be little question that Clearview violated BIPA, thereby infringing the privacy and security rights of Illinoisans. Yet Clearview argues that requiring it to comply with BIPA violates its First Amendment rights because its nonconsensual capture of faceprints from images is merely the analysis of public information, which it uses as a step in the process of running a search engine that republishes public information. As First Amendment advocates, amici take these claims seriously—but we disagree.

Capturing an individual's faceprint is conduct, not speech, and, absent consent, it is harmful. This holds whether a faceprint is captured from a live in-person scan or from publicly accessible images. Such harvesting is the equivalent of collecting people's fingerprints—whether by dusting physical spaces, or, closer to Clearview's technology, by extracting them from photographs[7]—and of collecting DNA from water bottles, coffee cups, or tissues discarded in public, all without notice or consent. Such conduct can be subject to consent requirements without violating the First Amendment.

[7] Such harvesting of fingerprints is not merely hypothetical. *See, e.g.*, Rob Picheta, *Drug Dealer Jailed After Sharing a Photo of Cheese that Included His Fingerprints*, CNN World (May 25, 2021), https://www.cnn.com/2021/05/25/uk/drug-dealer-cheese-sentenced-scli-gbr-intl/index.html; Olivia Solon, *The End of Passwords: Biometrics Are Coming But Do Risks Outweigh Benefits?*, The Guardian (Dec. 8, 2015), https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits; Robin Harding, *Fingerprint Theft Points to Digital Danger*, Fin. Times (Jan. 16, 2017), https://www.ft.com/content/446ac29a-dbc1-11e6-9d7c-be108f1c1dce.

A ruling to the contrary would make it virtually impossible for states to enact privacy and information security laws. Accepting that any use or dissemination of data is always fully protected speech "would jeopardize not just medical privacy rules, but most likely financial privacy rules, reader privacy rules," and "[a]rguably, even such venerable nondisclosure rules as the attorney-client duty of confidentiality." Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 Wm. & Mary L. Rev. 1501, 1522 (2015). *See also* Jane Bambauer, *Is Data Speech?*, 66 Stan. L. Rev. 57, 113–14 (2014) (recognizing that accepting this argument would likely signal the end for privacy protections like HIPAA and the Fair Credit Reporting Act). Proper application of the First Amendment does not produce this result.

This is not to say the First Amendment has no role in this case. Because BIPA has an incidental effect on Clearview's speech, it is subject to intermediate First Amendment scrutiny under *United States v. O'Brien*, 391 U.S. 367 (1968), and it survives that scrutiny. BIPA advances the state's substantial interests in protecting privacy and security, and it does not seek to suppress any expression.

For those reasons, amici urge the Court to deny Clearview's motion to dismiss.

ARGUMENT

Likening itself to a search engine that merely analyzes and republishes publicly available information, Clearview suggests that the First Amendment immunizes it from regulation. But this lawsuit challenges Clearview's conduct, not its speech. Clearview can gather information from the public internet and it can run a search engine without violating BIPA. What it cannot do is capture Plaintiffs' faceprints, or "scan[s] of . . . face geometry," 740 ILCS 14/10, without their knowledge or consent.

I. BIPA Regulates Conduct, Not Speech.

Far from viewing the capture of a faceprint as communication about or analysis of public information, courts applying BIPA have recognized that the nonconsensual capture of a person's biometric identifier is akin to "an act of trespass," *Bryant v. Compass Grp. USA*, 958 F.3d 617, 624 (7th Cir. 2020), and that "an invasion of an individual's biometric privacy rights has a close relationship to" traditional privacy torts, *Patel v. Facebook*, 932 F.3d 1264, 1273 (9th Cir. 2019) (citation and internal quotations omitted). Such activity is, and always has been, the subject of rules about consent, even when it may incidentally affect later speech. *See, e.g.*, *Lloyd Corp. v. Tanner*, 407 U.S. 551, 568 (1972) ("[T]his Court has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.").

The Supreme Court has recognized that this holds even for conduct—like "stealing documents or private wiretapping"—that deals largely in information, including potentially "newsworthy information." *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972). "It would be frivolous to assert . . . that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws . . . , whatever the impact on the flow of news." *Id.* In other words, the First Amendment does not guarantee access to all existing information. For example, the "willful[] intercept[ion of] . . . any wire or oral communication" is "unlawful conduct." *Bartnicki v. Vopper*, 532 U.S. 514, 523–24, 529 (2001).

Equally, not every use or analysis of amassed or publicly available information is protected speech—including, for example, fraud, identity theft, or the destruction of certain information. *See, e.g., United States v. Stevens*, 559 U.S. 460, 468 (2010) (First Amendment permits restrictions on "historic and traditional categories" of unprotected speech, including

fraud and speech integral to criminal conduct); *O'Brien*, 391 U.S. at 376 (destruction of draft card—that is, information within one's possession—is conduct, not speech).

Accepting Clearview's argument to the contrary would mean that acts like wiretapping, trespass, and identity theft—which equally involve the collection, analysis, or use of information—are fully protected expression, not conduct. And it would mean that collecting fingerprints in public places is unregulatable speech. That contention is so outlandish that it has not, to amici's knowledge, ever been raised in BIPA cases by any other defendant. *Cf. Rosenbach*, 2019 IL 123186, ¶ 33, 129 N.E. 3d at 1206 (holding that nonconsensual collection of fingerprints violates BIPA). Moreover, it runs the risk of allowing "an apparently limitless variety of conduct [to] be labeled 'speech.'" *O'Brien*, 391 U.S. at 376.

II. Faceprints Are Not Publicly Available Information.

BIPA's notice-and-consent requirement is not a downstream regulation of expression about information Clearview has lawfully acquired, but rather a regulation of the capture of a wholly new category of information. Clearview argues that "[c]entral to this case is the indisputable proposition that all information potentially relevant to this case is and has been publicly available." Def. MTD at 11. That proposition *is* central to this case—but, far from indisputable, it is incorrect. Information that is posted or exposed publicly is not the same as all information that might be acquired from it through additional action—including the capture of biometric identifiers. *Cf. Kyllo v. United States*, 533 U.S. 27, 35–37 (2001) (holding that the use of thermal imaging technology, even from outside a home, in order to extract information about the interior of a home constitutes a Fourth Amendment search, and expressly rejecting the argument that inferences drawn from publicly available information cannot be searches).

Courts have frequently recognized this difference when it comes to biological material. Even where, as Clearview argues is the case here, "one has consented to" share certain information about one's biology—be it a photograph or "blood or urine samples"—that "does not abolish one's privacy right not to be tested for intimate, personal matters." *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1270 (9th Cir. 1998). Rather, "[t]he ensuing . . . analysis . . . to obtain physiological data is a further invasion of the tested [person's] privacy interests." *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 616 (1989). Thus, even if Plaintiffs have consented to publication of photographs picturing them, they retain their privacy interests in their faceprints: the product of additional conduct performed to extract private information. To ignore this difference would be to hold that publishing a photograph of people's hands should be treated no differently than collecting their fingerprints.

Clearview's attempt to argue the contrary by analogizing itself to a search engine, relying on *Search King v. Google Tech.*, 2003 WL 21464568 (W.D. Okla. May 27, 2003), is unconvincing. Just as BIPA does not prohibit the republication of photographs, BIPA does not prohibit running a search engine—it merely prevents nonconsensually capturing faceprints, regardless of how they might subsequently be used. Clearview contends that *Search King* categorically holds "that the activities of search engines constitute speech entitled to First Amendment protection," Def. MTD at 11—but, in that case, the court recognized "the important distinction between process" (here, nonconsensual capturing of faceprints) "and result" (here Clearview's ranking of likely matches), and held only that the results "are constitutionally protected opinions." *Search King*, 2003 WL 21464568, at *3–4. Asserting that conduct is fully

protected speech because it ultimately helps to express an opinion proves too much.[8]

III. BIPA, Including as Applied to Clearview, Satisfies the First Amendment as a Regulation of Conduct Subject to Intermediate Scrutiny Under United States v. O'Brien.

At the same time, amici recognize that BIPA's notice-and consent requirement as applied to Clearview is not entirely free from First Amendment scrutiny. When "'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." *O'Brien*, 391 U.S. at 376; *see also Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 636 (1994) (applying *O'Brien* scrutiny to FCC rules that governed how "[c]able programmers and cable operators engage in and transmit speech"); *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 295 (1984) (upholding camping ban, though it burdened protests). Because BIPA has an incidental effect on Clearview's speech, specifically its expression of opinions about images, it is subject to intermediate scrutiny under *O'Brien*.

Under *O'Brien*, a regulation of conduct that incidentally burdens speech does not violate the First Amendment if the regulation "is within the constitutional power of the Government[,] if it furthers an important or substantial governmental interest [that] . . . is unrelated to the suppression of free expression," and "if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *O'Brien*, 391 U.S. at

[8] Neither does Clearview's use of code change the analysis. The mere fact that source code can be "an expressive means for the exchange of information and ideas," *see* Def. MTD at 11, does not mean that all uses of code are. At base, the same is true of words—while often protected by the First Amendment, they are also commonly regulated in ways that do not violate the First Amendment. *See e.g.*, *Stevens*, 559 U.S. at 468 (First Amendment permits restrictions on obscenity, defamation, fraud, incitement, and speech integral to criminal conduct). Plaintiffs challenge Clearview's capture of faceprints not because of the technological means that the company uses, but because of its conduct: the harvesting of biometric identifiers.

377. Here, BIPA is plainly within Illinois's power to enact, furthers substantial governmental interests in privacy and information security, is not aimed at suppression of free expression, and burdens Clearview's speech no more than is necessary to further those legitimate interests.

1. Illinois Has the Power to Regulate the Capture of Biometric Identifiers.

BIPA "is designed to protect consumers against the threat of irreparable privacy harms, identity theft, and other economic injuries." *Bryant*, 958 F.3d at 619; *see also Rosenbach*, 2019 IL 123186, ¶ 33, 129 N.E. 3d at 1206. Clearview does not contest the state's power to enact such a law.

2. BIPA Furthers Substantial Governmental Interests.

BIPA's notice-and-consent regime furthers the state's substantial interests in protecting its residents' privacy and security. Through BIPA, the General Assembly has properly "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 2019 IL 123186, ¶ 33, 129 N.E. 3d at 1206. Without BIPA, both of these rights would be violated at the moment that individuals' biometric identifiers are captured without their knowledge or consent—at that moment, "the right of [] individual[s] to maintain [their] biometric privacy vanishes into thin air" and "[t]he precise harm the Illinois legislature sought to prevent is then realized." *Id.*

In addition, BIPA furthers the state's interest in preventing the downstream harms enabled by the surreptitious and nonconsensual capture of biometric identifiers. Biometric identifiers can be used to enable access to other secure locations or information, including "to unlock the face recognition lock on [an] individual's cell phone," *Patel*, 932 F.3d at 1273, to keep time records at work, *Miller v. Sw. Airlines Co.*, 926 F.3d 898, 901 (7th Cir. 2019), and to determine entry to a gated space, *Rosenbach*, 2019 IL 123186, ¶ 4, 129 N.E. 3d at 1200.

Databases of sensitive biometrics—including the one maintained by Clearview—are therefore an inherent security hazard, as they can be subject to data breaches and employee misuse.

Once a faceprint is captured, a company can also use it to "identify [the] individual in any of the other hundreds of millions of photos uploaded [online] each day, as well as determine when the individual was present at a specific location." *Patel*, 932 F.3d at 1273. "[T]he facial-recognition technology at issue here can obtain information that is 'detailed, encyclopedic, and effortlessly compiled.'" *Id.*

Moreover, by protecting Illinoisans' privacy, the state protects *their* speech and associational rights. As the Supreme Court has recognized, "[f]ear or suspicion that one's speech is being monitored by a stranger"—for example, by someone using Clearview to track faces at a protest or political rally—"can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas." *Bartnicki*, 532 U.S. at 533. Equally, fear of monitoring can chill protected association, including associations at a house of worship, a domestic violence shelter, or an AA meeting. These state interests are "of the highest order." *Id.* at 518.

There is nothing speculative about the harms caused by nonconsensual capture of faceprints. For example, the Chinese government is amassing facial recognition databases of individuals who have mental illnesses, used drugs, or petitioned the government with grievances, and it is using face recognition to track and oppress the Uighur population.[9] Private companies in China have likewise developed face recognition technology that can purportedly identify and

[9] Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

track members of the Uighur minority.[10] Meanwhile, government agencies in the United States have used face recognition—including Clearview's technology—to surveil people exercising their First Amendment rights at protests.[11] American retail chains have surreptitiously used face recognition technology to identify shoppers, often in low-income neighborhoods and communities of color, resulting in harassment of shoppers who were deemed suspicious by the technology but in fact did nothing wrong.[12] A company that marketed itself as providing an online photo storage service secretly used millions of users' photos to train a face recognition algorithm, which it then sold to other private companies and government entities.[13] These and other well-established dangers of face recognition technology have led the world's largest professional computing society, ACM, to call for "an immediate suspension of the current and future private and governmental use of facial recognition (FR) technologies in all circumstances

---

[10] Drew Harwell & Eva Dou, *Huawei Tested AI Software that Could Recognize Uighur Minorities and Alert Police, Report Says*, Wash. Post (Dec. 8, 2020), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/; *Alibaba Facial Recognition Tech Specifically Picks Out Uighur Minority – Report*, Reuters (Dec. 17, 2020), https://www.reuters.com/article/us-alibaba-surveillance/alibaba-facial-recognition-tech-specifically-picks-out-uighur-minority-report-idUSKBN28R0IR.

[11] Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used to Identify Lafayette Square Protestor Accused of Assault*, Wash. Post (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html; Kate Cox, *Cops in Miami, NYC Arrest Protestors From Facial Recognition Matches*, ArsTechnica (Aug. 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches.

[12] Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, Reuters (July 28, 2020), https://www.reuters.com/investigates/special-report/usa-riteaid-software.

[13] Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools*, NBC News (May 9, 2019), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

known or reasonably foreseeable to be prejudicial to established human and legal rights" because the technology "has often compromised fundamental human and legal rights of individuals to privacy, employment, justice and personal liberty."[14]

Notwithstanding the unique privacy harms created by nonconsensual capture of biometric identifiers, Clearview argues that Plaintiffs lack any privacy interest in their faceprints because "individuals have no right to privacy in materials they post on the Internet." Def. MTD at 12. As discussed above, this conflates photographs and faceprints, ignoring the intrusive conduct required to capture the latter, and the unique privacy and security harms of such capture.[15]

3. The Government's Interests in BIPA Are Not Related to the Suppression of Free Expression.

BIPA proscribes nonconsensual faceprinting because it presents a privacy and security risk—not "*because* it has expressive elements." *Texas v. Johnson*, 491 U.S. 397, 406 (1989). Indeed, the conduct BIPA regulates often isn't used for expression at all. *See, e.g.*, *Miller*, 926 F.3d at 901 (capture of biometric identifiers used to keep time records at work); *Rosenbach*, 2019 IL 123186, ¶ 4, 129 N.E. 3d at 1200 (capture of biometric identifiers used to grant entry to a gated space).

Critically, if Clearview simply captured faceprints without consent and did not speak about or based on them at all, it would still violate BIPA.[16] Thus, the law "does not punish only

[14] Press Release, Ass'n for Computing Mach., *ACM US Technology Policy Committee Urges Suspension of Private and Governmental Use of Facial Recognition Technologies: Cites Potential for Injury from Bias to Society's Most Vulnerable Populations* (June 30, 2020), https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition-technologies.

[15] For this reason, the cases that Clearview cites regarding the lack of privacy interest in information posted to public social media pages are inapposite. *See* Def. MTD at 12 & n.9.

[16] It is worth noting that Clearview claims that the faceprints "are created within Clearview's search engine and are never made public . . . to anyone." Def. MTD at 10.

[conduct when] engaged in for the purpose of expressing views." *O'Brien*, 391 U.S. at 375. By the same token, BIPA's ban on nonconsensual capture of faceprints does not prevent anyone, including Clearview, from discussing the topic of identity or expressing their opinion regarding who appears to be in an image, regardless of what that opinion may be. Clearview can run a search engine for photographs without the nonconsensual capture of faceprints.

The law does not support Clearview's argument that BIPA is nevertheless content-based because it "attempts to burden [] efforts to identify people merely *because* [those efforts] are so effective," Def. MTD at 13.[17] For this proposition, Clearview relies on *Reed v. Town of Gilbert*, 576 U.S. 155 (2015) and *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361 (2018), two Supreme Court cases that hold that statutes are content-based if they "target speech based on its communicative content"—but, as discussed above, BIPA does not involve such targeting. Clearview's reliance on *Sorrell v. IMS Health* is equally misplaced. In *Sorrell*, the Supreme Court struck down a statute not because it diminished the effectiveness of speech, but because it "diminish[ed] the effectiveness of [speech]" *by a particular category of speakers* who "convey[ed] messages that are often in conflict with the goals of the state." 564 U.S. 552, 565 (2011) (internal quotations omitted). Thus, the case stands only for the uncontroversial point that regulations that target speech in a content- or viewpoint-based way are presumptively

[17] This argument is incorrect for the additional reason that, far from aiming to stifle innovation, Illinois enacted BIPA to build trust in biometric technology. *See* 740 ILCS 14/5(a), (e), (g) (legislative findings explaining that "[t]he use of biometrics . . . appears to promise streamlined financial transactions and security screenings," but that without effective regulation, "many members of the public are deterred from partaking in biometric identifier-facilitated transactions," and that "[t]he public welfare, security, and safety will be served by regulating the collection . . . of biometric identifiers").

unconstitutional.[18]

Clearview also argues that BIPA is a "speaker-based" restriction on speech because it exempts financial institutions and State contractors, and so must be subject to heightened First Amendment scrutiny under *Sorrell*.[19] But "[s]o long as they are not a subtle means of exercising a content preference, speaker distinctions of this nature are not presumed invalid under the First Amendment." *Turner*, 512 U.S. at 645; *see also id.* at 657 (rejecting contention that all speaker-based regulations are subject to strict scrutiny); *Reed*, 576 U.S. at 170 ("laws favoring some speakers over others demand strict scrutiny *when the legislature's speaker preference reflects a content preference*.") (emphasis added; marks and citation omitted). With respect to BIPA, there is no reason—nor does Clearview offer one—to presume that state contractors' or financial institutions' use of biometric identifiers will somehow reflect a content preference. Instead, just like other entities, state contractors and financial institutions might use biometric identifiers to decide whether an individual is an employee with access to a particular area, or to identify a person out on the street. In other words, to the extent that this reflects a "content" choice at all, it is choosing the same content.

[18] To the extent that Clearview argues that the law is content-based because it prevents it from using an "effective" (i.e., less "cumbersome") means of identifying people, this, too, misses the mark. Indeed, many of the regulations that courts have upheld under *O'Brien* regulate the effectiveness (or efficiency) of speech. For example, must-carry provisions prevent cable operators from allowing only a small subset of speakers to monopolize broadcasts. *Turner*, 512 U.S. at 661–63. Similarly, an Illinois court has held that an ordinance limiting sound volume—clearly a tool for efficiency of communication—is content-neutral. *People v. Arguello*, 327 Ill. App. 3d 984, 989, 765 N.E. 2d 98, 102–03 (1st Dist. 2002).

[19] It is worth noting that even *Sorrell* does not apply strict scrutiny, instead holding that the statute fails scrutiny requiring that it "directly advance[] a substantial governmental interest and that the measure is drawn to achieve that interest." 564 U.S. at 572. Because the statute failed this intermediate scrutiny, the Supreme Court declined "to determine" whether "a stricter form of judicial scrutiny" must be satisfied. *Id.* at 571.

Indeed, the Supreme Court held that the law prohibiting disclosure of wiretapped conversations at issue in *Bartnicki v. Vopper* was content neutral, 532 U.S. at 526, notwithstanding the law's exceptions for officers, employees, and agents of the Federal Communications Commission and communication services, and operators of switchboards, 18 U.S.C. § 2511(2)(a)(i), (b). *Cf. Sorrell*, 564 U.S. at 573 (recognizing that a First Amendment challenge to a more coherent privacy policy "would present quite a different case"). It is common for lawmakers to enact separate statutes to regulate private and governmental access to private information, but that does not leave the regulation of private actors vulnerable to First Amendment challenge. *Compare, e.g.*, 47 U.S.C. § 222 (requiring customer consent before telecommunications carriers can disclose cell phone location information and other sensitive data, "[e]xcept as required by law"), *with* 18 U.S.C. § 2703 (permitting nonconsensual law enforcement access to such records, but only pursuant to subpoena, court order, or warrant).

4. The Incidental Restriction on Speech Is No Greater than Is Essential to Further the Government's Interests.

Finally, the notice and consent requirement does "not burden substantially more speech than is necessary to further the government's legitimate interests." *Turner*, 520 U.S. at 662 (citation and internal quotations omitted). Even though "a regulation need not be the least-restrictive means of advancing the Government's interests" to satisfy intermediate scrutiny, *id.*, BIPA's notice-and-consent requirement targets "[t]he precise harm the Illinois legislature sought to prevent." *Rosenbach*, 2019 IL 123186, ¶ 34, 129 N.E. 3d at 1206. It "insure[s] that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised," which is essential in light of the "difficulty in providing meaningful recourse once a person's biometric identifiers or biometric information has been compromised." *Id.* ¶ 36,

129 N.E. 3d at 1206–07. Much like the ban on destroying draft cards at issue in *O'Brien*, BIPA "prohibits [the harmful] conduct and does nothing more." 391 U.S. at 381–82. "To require individuals to wait until they have sustained some compensable injury . . . before they may seek recourse . . . would be completely antithetical to the Act's preventative and deterrent purposes." *Rosenbach* 2019 IL 123186, ¶ 37, 129 N.E. 3d at 1207.

The legislative record demonstrates a careful balancing of interests, and one that results in a person's "power to say no" before their immutable identifiers are taken from them. *Rosenbach*, 2019 IL 123186, ¶ 34, 129 N.E. 3d at 1206. As the Illinois Supreme Court has noted, "whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced. That is the point of the law." *Id.* ¶ 37, 129 N.E. 3d at 1207.

Moreover, rather than impose an absolute ban on faceprinting, BIPA allows faceprinting with an individual's consent. This approach, which "is not absolute," *Boelter v. Hearst Commc'ns*, 192 F. Supp. 3d 427, 449 (S.D.N.Y. 2016), is "narrowly drawn" because "it permits [capture] for any reason with the [individual's] permission," *Boelter v. Advance Magazine Publishers, Inc.*, 210 F. Supp. 3d 579, 602 (S.D.N.Y. 2016). *See also Nat'l Cable & Telecomms., Ass'n v. FCC*, 555 F.3d 996, 1001–02 (D.C. Cir. 2009) (holding that FCC rule requiring opt-in consent was sufficiently tailored to survive intermediate First Amendment scrutiny). Under BIPA, there is no liability for the dissemination of the very same biometric identifier obtained and distributed with consent.[20]

[20] For the same reasons, BIPA is not overbroad. Clearview argues that BIPA is overbroad because it bars Clearview from matching published photographs with other photographs. But

CONCLUSION

For the foregoing reasons, Clearview's motion to dismiss on First Amendment grounds should be denied.

Dated: July 9, 2021

Respectfully submitted,

By: /s/ Rebecca K. Glenberg

Vera Eidelman
veidelman@aclu.org
Nathan Freed Wessler
nwessler@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, New York 10004
Tel: 212.549.2500

Jay Edelson
jedelson@edelson.com
Benjamin H. Richman
brichman@edelson.com
David I. Mindell
dmindell@edelson.com
J. Eli Wade-Scott
ewadescott@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370

Attorneys for Amicus Curiae American Civil Liberties Union

Rebecca K. Glenberg
rglenberg@aclu-il.org
ROGER BALDWIN FOUNDATION OF ACLU, INC.
150 North Michigan Avenue, Suite 600
Chicago, Illinois 60601
Tel: 312.201.9740

Attorney for Amici Curiae American Civil Liberties Union and American Civil Liberties Union of Illinois

BIPA only bans Clearview from doing so by relying on biometric identifiers that Clearview unlawfully captured without notice or consent. Clearview has failed to identify protected speech that is banned by BIPA—only speech that is incidentally burdened by it.